METHOD FOR GENERATION, DELIVERY, AND VALIDATION OF ELECTRONIC COUPONS THROUGH PERSONAL TV SERVICE SYSTEM

BACKGROUND OF THE INVENTION

TECHNICAL FIELD

The invention relates to prosecution of electronic coupons using telecommunication technology. More particularly, the invention relates to a process and methods for generation, delivery, and validation of electronic coupons through a personal television service system.

DESCRIPTION OF THE PRIOR ART

Traditionally, a coupon is a certificate that one can use to buy a product or service at a reduced price or to get it free, or to get information, used by businesses as a way to make their name more widely known or to encourage sales. The coupons are usually printed objects, carrying printed indicia or a coupon number to prevent forgery. Printed coupons are issued and distributed via newspapers, magazines, flyers or other publications. To redeem a coupon, the coupon holder needs to surrender the coupon to the vendor and the vendor examines the coupon to verify by the printed indicia whether or not the coupon is valid. Upon successful verification, the vendor provides the goods or services to the customer, and then collects the coupon to remove it from circulation.

The printed coupons may be redeemed remotely through a central electronic coupon management facility wherein a database containing information for valid coupons communicates with a plurality of remote terminals, enabling telecommunications operators to verify or validate a coupon in real-time. Each coupon in the database has a unique coupon number that is cryptographically transformed when released to a customer. A plurality of operator consoles are linked to the coupon management facility and can request verification, validation and other processing of the coupons. In operation, a customer communicates with an operator located at one of the operator consoles, and reads the cryptographic coupon number on an issued coupon to the operator. The operator uses the operator console to communicate the coupon information to the coupon management facility. A message is returned to the operator indicating the status of the coupon. If the coupon is available, the operator provides the customer the goods or services authorized via the coupon.

A coupon may be generated in electronic form and issued via telecommunication means such as television or Internet. With the advent of personal television service (PTVS), through which a TV viewer may access to a centralized TV program guide database and program his digital video recorder anywhere, it has been realized that PTVS system would be a good channel to issue coupons to TV viewers.

Therefore, there is a need to develop a process for generating, delivering, and validating electronic coupons through a personal TV service system or similar telecommunication system with a higher security and convenience.

SUMMARY OF THE INVENTION

A process for coupon generation, delivery, and validation over a personal TV service (PTVS) system is disclosed. According to this invention, a client issues electronic coupons to one or more personal TV service customers through a personal TV service center. The coupon must be validated before a coupon is redeemed at any designated vendor or retail stores that accesses to the personal TV service center.

The present invention provides a cryptographic basis for coupon generation and validation. The invention utilizes the current crypto-chip built in each personal TV service receiver without changing its architecture. The personal TV service center generates one or more random coupon authentication numbers for each receiver. The coupon authentication numbers are known to the key server, the coupon validation number database, and the receiver in encrypted form as private keys. The receiver also has various public keys, one of which is its product serial number. This serial number is known to both the owner and the personal TV service center.

For each offer (coupon content), a unique offer ID number is designated either by the client or by the personal TV service center. The receiver performs a hash operation on the offer ID number using the coupon authentication number, and takes the first or last 6 digits of the hashed result as a coupon ID number. Thus each coupon comprises three numbers: an offer ID number representing a specific product or service, a receiver serial number representing the receiver owner (usually the coupon holder), and a coupon ID number representing this specific coupon. The customer may take these three

numbers to a vendor and redeem the coupon or redeem the coupon remotely through an electronic coupon management system.

Before the coupon is redeemed, it must be validated. To validate the coupon, the personal TV service center uses the receiver serial number as the public key to look up the coupon authentication number stored in the database, and performs a hash operation on the offer ID number using the authentication number. The key server takes the first or the last 6 digits of the hashed result and compares this number with the coupon ID number submitted by the customer. If these two numbers match, the coupon is validated.

The present invention enables secure distribution and validation of coupons using the personal TV service system without need to change the current receivers' hardware infrastructure. The advantages and benefits of this invention are numerous. For example, it minimizes the amount of work involved to issue electronic coupons; the offer ID numbers and coupons ID numbers are flexible and short enough that a consumer can write them down easily on a piece of paper; these numbers are highly unpredictable and it is very difficult to crack them via brute-force methods.

BRIEF DESCRIPTION OF THE DRAWINGS

Fig. 1 is a block diagram illustrating a coupon distribution and encryption system;

Fig. 2 is a data flow control diagram illustrating a process for coupon authentication number generation;

Fig. 3 is a data flow control diagram illustrating a process for coupon delivery; and

Fig. 4 is a data flow diagram illustrating a process for coupon verification.

DETAILED DESCRIPTION OF THE INVENTION

In the following detailed description of the invention, some specific details are set forth to provide a thorough understanding of the presently preferred embodiment of the invention. However, it will be apparent to those skilled in the art that the invention may be practiced in embodiments that do not use the specific details set forth herein. Well known methods, procedures, components, and circuitry have not been described in detail.

In the following discussion, in references to the drawings like numerals refer to like parts throughout the several views.

Figure 1 is a block diagram that illustrates a coupon distribution system 100. The preferred embodiment of this system comprises a client 105 which issues electronic coupons, a personal TV service (PTVS) center 110, a personal TV service (PTVS) receiver 130 which may be a personal video recorder, and a TV set 145 that displays TV programs and coupons. The PTVS center 110 comprises a receiver activation database 115, a coupon authentication number database 116 and a key server 120. The PTVS receiver 130 comprises a crypto-chip 135 and a hard drive 140.

The PTVS center 110 sends encrypted electronic coupons issued by the client 105 to the PTVS receiver 130 through a communication channel 125, which may be a telephone modem, a cable modem, or a local area network (LAN). Each PTVS receiver is assigned various public keys, one of which is the serial number of that receiver. The public keys are stored in the hard drive 140 of the PTVS receiver 130 and are also stored in the receiver activation database 115 in the PTVS center 110. One or two private keys are assigned to each PTVS receiver, which are stored in the crypto-chip 135 of the PTVS receiver 130.

The operation of the coupon distribution system 100 includes three processes:

- process for coupon authentication number generation;
- process for coupon delivery; and
- process for coupon validation.

A. Process For Coupon Authentication Number Generation

Figure 2 is a data flow control diagram that illustrates a process 200 for coupon authentication number generation for each PTVS receiver. The process 200 comprises the steps of:

Step 210: The PTVS center 110 activates the PTVS receiver 130.

Step 220: Upon activation, the PTVS center 110 generates a coupon authentication number for the PTVS receiver. This coupon authentication

number is randomly given and can be of any size up to 512 bits long or longer.

Step 230: The PTVS center 110 saves the coupon authentication number in the coupon authentication number database 116.

Step 240: The PTVS center 110 communicates the coupon authentication number to the PTVS key server 120.

Step 250: When the PTVS receiver 130 contacts the PTVS center 110 first time or next time, the PTVS key server 120 perceives that the PTVS receiver 130 has not yet had a coupon master key and then it encrypts the coupon authentication number using the PTVS receiver's El Gamal public key which is stored both in the receiver activation database 115 and in the PTVS receiver's hard drive 140.

Step 260: The key server 120 sends the encrypted coupon authentication number to the PTVS receiver 130 which adds the encrypted authentication number as an encrypted coupon key to its keyring. A date or time stamp may be embedded in the coupon key for convenience if the coupon validation number database 116 is ever compromised.

The process 200 for coupon authentication number generation takes 1-2 CPU seconds per PTVS receiver and needs to be done only once unless the coupon authentication number database 116 is compromised.

B. Process For Coupon Delivery

Figure 3 is a data flow control diagram that illustrates a process 300 for coupon delivery. The process 300 comprises the steps of:

Step 310: The PTVS center 110 receives an order from the client 105 to issue an electronic coupon, which is an offer to sell a specific product or service.

The client 105 may generate or acquire a unique offer ID number and communicate this offer ID number to the PTVS center 110. The offer ID number may be up to 512 bits in length. However, 32 bits is usually adequate and allows for a numeric encoding to identify the client and the offer. The offer ID number may also be implemented as ASCII character strings of up to 64 bytes.

Step 320: The PTVS center 110 checks whether or not the client 105 has generated an ID number for the offer.

Step 330: If the ID number exists, the PTVS center 110 checks the uniqueness of the ID number and resolves possible collisions with other offers.

Step 340: If the ID number does not exist, the PTVS center 110 creates a unique ID number for the offer. As described above, the offer ID number may be up to 512 bits in length and may also be implemented as ASCII character strings of up to 64 bytes.

Step 350: The PTVS center sends the offer ID number and coupon information to the TV set 145 through the PTVS receiver 130.

Step 360: Upon receipt of the coupon, the customer decides to accept or reject the offer.

Step 370: If the customer accepts the offer, the crypto-chip 135 in the PTVS receiver 130 performs a hash operation on the offer ID number using the

coupon authentication number. Here, the PTVS receiver 130 uses its crypto-chip 135 to first decrypt the coupon authentication number yielding a number decryptedAuthencator and then perform a hash operation of SHA1(offerID^decryptedAuthencator). The hashed result is SHA1RESULT.

Step 380: The PTVS receiver takes the first 6 digits of the hashed result as a coupon ID number. Here, the PTVS receiver 130 treats SHA1RESULT as an integer, and calculates the coupon ID number as being (SHA1RESULT mod Intc), where Intc is a convenient integer of probably 10 ^ 6 or so, yielding a 6-digit coupon ID, which is the first 6 digits of SHA1RESULT.

This process takes 10-15 seconds. The PTVS receiver 130 may either put up a stopwatch icon, or display a screen giving detailed instruction about how the user can redeem the coupon.

C. Process For Coupon Validation

Figure 4 is a data flow diagram that illustrates a process 400 for coupon validation. The process 400 comprises the steps of:

Step 410: The customer submits the offer ID, the coupon ID, and the receiver serial number to a vendor.

Step 420: The vendor accesses to a Common Gateway Interface (CGI) at the PTVS center 110 and inputs the offer ID, the coupon ID, and the receiver serial number.

Step 430: The key server 120 looks up the unencrypted coupon authentication number from the coupon validation number database 116.

Step 440: The key server 120 uses the unencrypted authentication number as a key and performs a hash operation on the offer ID number as Step 370.

Step 450: The key server 120 takes the first 6 digits of the hashed result and compares this 6-digit number with the coupon ID number submitted by the customer. If these two numbers match, the coupon is validated.

Because SHA1 is highly unpredictable, it is very difficult to crack these numbers via brute-force methods. The reliability of these processes in terms of security depends on the coupon validation number database and the coupon ID size. If somebody breaks into the validation machine and siphons off the database, he could steal the validation numbers for all receivers and forge coupons at will. However, this can be prevented by keeping the validation machine behind a firewall and strictly limit the sorts of access permitted. In case there is a security leak, the service center will first fix the leak and then regenerate new coupon authentication numbers for all receivers and distribute them via the key server.

If the coupon ID is too small, for example, 3-4 digits, it becomes possible to generate coupon ID numbers by brute force. This can be prevented by generating coupon ID numbers with adequate length. In actuality, 5-6 digits would be good enough.

Although the invention is described herein with reference to the preferred embodiment, one skilled in the art will readily appreciate that other applications may be substituted for those set forth herein without departing from the spirit and scope of the present invention.

Accordingly, the invention should only be limited by the Claims included below.